

TINDAK PIDANA CYBER CRIME DALAM PERSPEKTIF  
UNDANG – UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI  
DAN TRANSAKSI ELEKTRONIK

SKRIPSI

Diajukan untuk memenuhi sebagai persyaratan memperoleh Gelar Sarjana  
Hukum pada Fakultas Hukum UPN “Veteran” Jawa Timur



Oleh :

GINANJAR SAPTO HADI  
0771010121

YAYASAN KESEJAHTERAAN PENDIDIKAN DAN PERUMAHAN  
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAWA TIMUR  
FAKULTAS HUKUM PROGRAM STUDI ILMU HUKUM  
SURABAYA  
2012

PERSETUJUAN MENGIKUTI UJIAN SKRIPSI

TINDAK PIDANA CYBER CRIME DALAM PERSPEKTIF UNDANG –  
UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN  
TRANSAKSI ELEKTRONIK

Disusun Oleh :

Ginanjari Sapto Hadi  
NPM. 0771010121

Telah disetujui untuk mengikuti Ujian Skripsi

Menyetujui,

Pembimbing Utama

Pembimbing Pendamping

Subani, SH., M.Si.  
NIP. 19510504 198303 1 001

Yana Indawati, SH., M.Kn.  
NPT. 3 7901 07 0224

Mengetahui  
D E K A N

Hariyo Sulistiyantoro, SH, MM  
NIP. 19 6206 25199 1031 001

PERSETUJUAN DAN PENGESAHAN REVISI SKRIPSI  
TINDAK PIDANA CYBER CRIME DALAM PERSPEKTIF UNDANG –  
UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN  
TRANSAKSI ELEKTRONIK

Oleh :

Ginanjari Sapto Hadi  
NPM. 0771010121

Telah dipertahankan dihadapan dan diterima oleh Tim Penguji Skripsi  
Program Studi Ilmu Hukum Fakultas Hukum  
Universitas Pembangunan Nasional “Veteran” Jawa Timur  
Pada tanggal 07 Juni 2012  
Menyetujui,

Pembimbing Utama

Tim Penguji :

1.

Subani, SH., M.Si.  
NIP. 195105041983031001

Sutrisno, S.H., M.Hum  
NIP. 196012121988031001

2.

Pembimbing Pendamping

Subani, SH., M.Si.  
NIP. 195105041983031001

Yana Indawati, SH., M.Kn.  
NPT. 37901070224

3.

Hariyo Sulistyantoro, SH, MM  
NIP. 196206251991031001

Mengetahui  
D E K A N

Hariyo Sulistyantoro, SH, MM  
NIP. 196206251991031001

PERSETUJUAN DAN PENGESAHAN REVISI SKRIPSI  
TINDAK PIDANA CYBER CRIME DALAM PERSPEKTIF UNDANG –  
UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN  
TRANSAKSI ELEKTRONIK

Oleh :

Ginanjari Sapto Hadi  
NPM. 0771010121

Telah dipertahankan dihadapan dan diterima oleh Tim Penguji Skripsi  
Program Studi Ilmu Hukum Fakultas Hukum  
Universitas Pembangunan Nasional “Veteran” Jawa Timur  
Pada tanggal 07 Juni 2012  
Menyetujui,

Pembimbing Utama

Tim Penguji :

1.

Subani, SH., M.Si.  
NIP. 195105041983031001

Sutrisno, S.H., M.Hum  
NIP. 196012121988031001

2.

Pembimbing Pendamping

Yana Indawati, SH., M.Kn.  
NPT. 37901070224

Subani, SH., M.Si.  
NIP. 195105041983031001

3.

Hariyo Sulistiyantoro, SH, MM  
NIP. 196206251991031001

Mengetahui  
D E K A N

Hariyo Sulistiyantoro, SH, MM  
NIP. 196206251991031001

## SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama : Ginanjar Sapto Hadi  
Tempat/ Tgl lahir : Sidoarjo, 29 Agustus 1987  
NPM : 0771010121  
Konsentrasi : Pidana  
Alamat : Perum Kraton Harmoni blok B7/11 Pasuruan

Menyatakan dengan sebenarnya bahwa skripsi saya dengan judul :  
“TINDAK PIDANA CYBER CRIME DALAM PERSPEKTIF UNDANG –  
UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN  
TRANSAKSI ELEKTRONIK” dalam rangka memnuhi syarat untuk  
memperoleh gelar Sarjana Hukum pada Fakultas Hukum Universitas  
Pembangunan Nasional “Veteran” Jawa Timur adalah benar – benar hasil karya  
cipta saya sendiri, yang saya buat sesuai dengan ketentuan yang berlaku, bukan  
hasil jiplakan (plagiat).-----

Apabila di kemudian hari ternyata skripsi ini hasil jiplakan (plagiat) maka  
saya bersedia dituntut di depan pengadilan dan dicabut gelas kesarjanaan (Sarjana  
Hukum) yang saya peroleh.-----

Demikian surat pernyataan ini saya buat dengan sebenar – benarnya  
dengan penuh rasa tanggung jawab atas segala akibat hukumnya.-----

Mengetahui  
Pembimbing Utama

Surabaya, 20 Mei 2012  
Penulis

Subani, SH., M.Si.  
NIP. 195105041983031001

Ginanjar Sapto Hadi  
NPM. 0771010121

## KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Alhamdulillah, puji syukur Kehadirat Allah SWT yang telah memberi rahmat dan hidayahNya, sehingga penulis dapat menyelesaikan Skripsi dengan judul “TINDAK PIDANA CYBER CRIME DALAM PERSPEKTIF UNDANG - UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK”.

Dalam menyelesaikan Skripsi ini, penulis menyadari sepenuhnya bahwa selesainya penyusunan Skripsi ini tidak lepas dari bantuan berbagai pihak, untuk itu dalam kesempatan ini penulis mengucapkan terima kasih kepada:

1. Bapak Hariyo Sulistiyantoro, S.H., M.M. selaku Dekan Fakultas Hukum Universitas Pembangunan Nasional “Veteran” Jawa Timur.
2. Bapak H.Sutrisno, S.H., M.Hum selaku Wakil Dekan I Fakultas Hukum Universitas Pembangunan Nasional “Veteran” Jawa Timur.
3. Bapak Drs. Ec. Gendut Soekarno, M.S. selaku Wakil Dekan II Fakultas Hukum Universitas Pembangunan Nasional “Veteran” Jawa Timur.
4. Bapak Subani, S.H., M.Si. selaku Ketua Program Studi Fakultas Hukum Universitas Pembangunan Nasional “Veteran” Jawa Timur.
5. Bapak Subani, S.H., M.Si. selaku Dosen Pembimbing Utama yang selalu memberikan pengarahan dan bimbingan selama pengerjaan Skripsi.
6. Ibu Yana Indawati, S.H., M.Kn. selaku Dosen Pembimbing Pendamping yang selalu memberikan pengarahan dan bimbingan selama pengerjaan Skripsi.
7. Ibu Wiwin Yulianingsih, S.H., M.Kn. selaku Dosen Wali yang telah memberikan bekal ilmu serta nasehatnya kepada penulis selama menempuh

studi di Fakultas Hukum Universitas Pembangunan Nasional “Veteran” Jawa Timur.

8. Kedua orang tua, Drs. Sufyan Hadi, S.sos Bapakku dan Reny Setyowati Ibuku yang selalu memberi semangat dan curahan kasih sayang tanpa henti dan telah mendukung secara moril maupun materiil.
9. Teman-teman seperjuangan Adi Kurnia Pratama Putra, Yudha Prinata, Wimar Sasongko, Chandra, Wahana, Dody Fajar, serta segenap dosen, staff juga mahasiswa Fakultas Hukum angkatan 2007 Universitas Pembangunan Nasional “Veteran” Jawa Timur yang belum disebutkan satu persatu.
10. Terakhir, untuk calon pendamping hidupku Ayu Fitriana, S.KM yang selalu menemani dan mendukung penulis agar menyelesaikan Skripsi.

Penulis menyadari bahwa penulisan Skripsi ini masih jauh dari sempurna dan penuh keterbatasan. Dengan harapan bahwa Skripsi ini Insya Allah akan berguna bagi rekan-rekan di Program Studi Ilmu Hukum, maka saran serta kritik yang membangun sangatlah dibutuhkan untuk memperbaiki kekurangan yang ada.

Surabaya, 07 Juni 2012

Penulis

## DAFTAR ISI

HALAMAN JUDUL .....	i
HALAMAN PERSETUJUAN .....	ii
HALAMAN PENGESAHAN .....	iii
HALAMAN SURAT PERNYATAAN KEASLIAN .....	iv
KATA PENGANTAR .....	v
DAFTAR ISI .....	vii
ABSTRAK .....	ix
BAB I    PENDAHULUAN .....	1
A. Latar Belakang .....	1
B. Rumusan Masalah .....	6
C. Tujuan Penulisan .....	6
D. Manfaat Penulisan .....	7
E. Kajian Pustaka .....	7
F. Metode Penelitian .....	26
G. Sistematika Penulisan .....	29
BAB II   PELAKSANAAN UU ITE TERHADAP TINDAK PIDANA CYBER CRIME .....	31
A. Proses terjadinya Cyber crime .....	31
B. Prosedur penanganan di kepolisian .....	33
C. Analisa pelaksanaan UU ITE terhadap Tindak Pidana Cyber crime .....	36



BAB III	SISTEM PEMBUKTIAN TINDAK PIDANA CYBER CRIME	
	A. Proses pembuktian terhadap tindak pidana Cyber crime .....	39
	B. Beberapa contoh kasus Tindak Pidana Cyber Crime.....	44
BAB IV	PENUTUP .....	50
	A. Kesimpulan.....	50
	B. Saran .....	51
DAFTAR PUSTAKA .....		53

UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAWA TIMUR  
FAKULTAS HUKUM

Nama Mahasiswa : Ginanjar Sapto Hadi  
NPM : 0771010121  
Tempat Tanggal Lahir : Sidoarjo, 29 Agustus 1987  
Program Studi : Strata 1 (S1)  
Judul Skripsi :

TINDAK PIDANA CYBER CRIME DALAM PERSPEKTIF UNDANG –  
UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN  
TRANSAKSI ELEKTRONIK

ABSTRACT

This study aims to determine the implementation of the Act - Act No. 11 of 2008 on Information and Electronic Transactions. This study uses a normative juridical. Source of data obtained from the literature and applicable legislation. Analysis of data using a normative juridical approach and conduct interviews. The results can be summarized research If the verification process conducted by a team of police did not find evidence of the case file can not be complete or P21 then the file can not be delegated to the court but in the process of proof on Cyber crime case can certainly be done by submitting documentary evidence form of electronic documents that can be implemented directly in the trial with the results of a print out or electronic documents. It is found in Article 5 paragraph (1) of ITE. In the implementation of UU ITE on Indonesia in accordance with the provisions of statutory law and regulations regarding the application of appropriate sanctions and threats to the acts committed by criminal cyber crime. The police and the state in order to explore the science that has been developed and are experts in dealing with cases of cyber crime. And the importance of the knowledge given to the general public to take extra - careful in performing all acts relating to the internet.

Keywords: Criminal Offenses, Cyber Crime, The Electronic Transactions.

UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAWA TIMUR  
FAKULTAS HUKUM

Nama Mahasiswa : Ginanjar Sapto Hadi  
NPM : 0771010121  
Tempat Tanggal Lahir : Sidoarjo, 29 Agustus 1987  
Program Studi : Strata 1 (S1)  
Judul Skripsi :

TINDAK PIDANA CYBER CRIME DALAM PERSPEKTIF UNDANG –  
UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN  
TRANSAKSI ELEKTRONIK

**ABSTRAKSI**

Penelitian ini bertujuan untuk mengetahui pelaksanaan Undang – Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Penelitian ini menggunakan metode yuridis normatif. Sumber data yang diperoleh dari literatur dan perundang-undangan yang berlaku. Analisa data menggunakan pendekatan yuridis normatif dan melakukan wawancara. Hasil penelitian dapat disimpulkan Apabila dalam proses pembuktian yang dilakukan oleh tim dari kepolisian tidak menemukan bukti maka berkas kasus tidak dapat lengkap atau P21 maka berkas tersebut tidak dapat dilimpahkan ke pengadilan tetapi dalam proses pembuktian pada perkara Cyber crime ini tentu saja dapat dilakukan dengan mengajukan bukti surat berupa dokumen elektronik yang dapat dilaksanakan langsung di persidangan dengan hasil berupa print out atau dokumen elektronik. Hal tersebut terdapat pada Pasal 5 ayat (1) UU ITE. Dalam pelaksanaan UU ITE di Indonesia sesuai dengan ketentuan perundang undangan yang berlaku mengenai penerapan sanksi dan ancaman yang sesuai dengan perbuatan yang dilakukan oleh pelaku tindak pidana Cyber crime. Serta Pihak kepolisian supaya menggali ilmu ke negara yang sudah maju dan sudah ahli dalam mengatasi kasus Cyber crime. Serta pentingnya pengetahuan diberikan kepada masyarakat awam agar lebih berhati - hati dalam melakukan segala tindakan yang berhubungan dengan internet.

Kata Kunci : Tindak pidana, Cyber crime, Transaksi Elektronik.

# BAB I

## PENDAHULUAN

### A. Latar Belakang Masalah

Keunggulan komputer berupa kecepatan dan ketelitiannya dalam menyelesaikan pekerjaan sehingga dapat menekan jumlah tenaga kerja, biaya serta memperkecil kemungkinan melakukan kesalahan, mengakibatkan masyarakat semakin mengalami ketergantungan kepada komputer. Dampak negatif dapat timbul apabila terjadi kesalahan yang ditimbulkan oleh peralatan komputer yang akan mengakibatkan kerugian besar bagi pemakai atau pihak-pihak yang berkepentingan. Kesalahan yang disengaja mengarah kepada penyalahgunaan komputer.<sup>1</sup>

Usaha mewujudkan cita-cita hukum untuk mensejahterakan masyarakat melalui kebijakan hukum pidana tidak merupakan satu-satunya cara yang memiliki peran paling strategis. Dikatakan demikian karena hukum pidana hanya sebagai salah satu dari sarana kontrol masyarakat.

Teknologi informasi dan komunikasi telah mengubah perilaku masyarakat dan peradaban manusia secara global. Di samping itu, perkembangan teknologi informasi telah menyebabkan dunia menjadi tanpa batas dan menyebabkan perubahan sosial yang secara signifikan berlangsung demikian cepat. Teknologi informasi saat ini sangat berarti dalam memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan

---

<sup>1</sup> <http://www.scribd.com/doc/11654767/tinjauan-yuridis-pembuktian-cyber-crime-dalam-perspektif-hukum-positif-indonesia>, 21 November 2011, 15.00 wib.

dan peradaban manusia, sekaligus menjadi arena efektif perbuatan melawan hukum.

Saat ini telah lahir suatu rezim hukum baru yang dikenal dengan Hukum siber, yang diambil dari kata Cyber Law adalah istilah hukum yang terkait dengan pemanfaatan teknologi informasi. Istilah lain yang digunakan adalah Hukum Teknologi Informasi (Law Of Information Technology), Hukum Dunia Maya (Virtual World Law). Istilah - istilah tersebut lahir mengingat kegiatan internet dan pemanfaatan teknologi informasi berbaris virtual. Istilah hukum siber digunakan dalam tulisan ini dilandasi pemikiran bahwa cyber jika diidentikan dengan "Dunia Maya" akan cukup menghadapi persoalan jika harus membuktikan suatu persoalan yang diasumsikan sebagai "maya", sesuatu yang tidak terlihat dan semu.

Terdapat tiga pendekatan untuk mempertahankan keamanan di cyberspace, pertama adalah pendekatan teknologi, kedua pendekatan sosial budaya-etika, dan ketiga pendekatan hukum. Untuk mengatasi keamanan gangguan pendekatan teknologi sifatnya mutlak dilakukan, sebab tanpa suatu pengamanan jaringan akan sangat mudah disusupi, diintersepsi, atau diakses secara ilegal dan tanpa hak.

Melihat fakta hukum sebagaimana yang ada pada saat ini, dampak perkembangan ilmu pengetahuan dan teknologi yang telah disalahgunakan sebagai sarana kejahatan ini menjadi teramat penting untuk diantisipasi bagaimana kebijakan hukumnya, sehingga Cyber crime yang terjadi dapat dilakukan upaya penanggulangannya dengan hukum pidana, termasuk dalam hal ini adalah mengenai sistem pembuktiannya.

Dikatakan teramat penting karena dalam penegakan hukum pidana dasar pembenaran seseorang dapat dikatakan bersalah atau tidak melakukan tindak pidana, di samping perbuatannya dapat dipersalahkan atas kekuatan Undang-undang yang telah ada sebelumnya (asas legalitas), juga perbuatan mana didukung oleh kekuatan bukti yang sah dan kepadanya dapat dipertanggungjawabkan (unsur kesalahan). Pemikiran demikian telah sesuai dengan penerapan asas legalitas dalam hukum pidana (KUHP) kita, yakni sebagaimana dirumuskan secara tegas dalam Pasal I ayat (1) KUHP " *Nullum delictum nulla poena sine praevia lege poenali*" atau dalam istilah lain dapat dikenal, " tiada pidana tanpa kesalahan".

Bertolak dari dasar pembenaran sebagaimana diuraikan di atas, bila dikaitkan dengan Cyber crime, maka unsur membuktikan dengan kekuatan alat bukti yang sah dalam hukum acara pidana merupakan masalah yang tidak kalah pentingnya untuk diantisipasi di samping unsur kesalahan dan adanya perbuatan pidana. Akhirnya dengan melihat pentingnya persoalan pembuktian dalam Cyber crime, skripsi ini hendak mendeskripsikan pembahasan dalam fokus masalah Hukum Pembuktian terhadap Cyber crime dalam Hukum Pidana Indonesia.

Oleh karena alasan - alasan tersebut di atas, bagaimana pembuktian - pembuktian dalam Cyber crime cukup sulit dilakukan mengingat, bahwa hukum di Indonesia yang mengatur masalah ini masih banyak cacat hukum yang dapat dimanfaatkan oleh para pelaku Cyber crime untuk lepas dari proses pemidanaan.

Bentuk-bentuk Cyber crime pada umumnya yang dikenal dalam masyarakat dibedakan menjadi 3 (tiga) kualifikasi umum yaitu<sup>2</sup> :

- 1).Kejahatan Dunia Maya yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer.
  - a). Illegal access (akses secara tidak sah terhadap sistem komputer).
  - b). Data interference (mengganggu data komputer).
  - c). System interference (mengganggu sistem komputer).
  - d). Illegal interception in the computers, systems and computer networks operation (intersepsi secara tidak sah terhadap komputer, sistem, dan jaringan operasional komputer).
  - e). Data Theft (mencuri data).
  - f). Data leakage and espionage (membocorkan data dan memata-matai).
  - g). Miss use of devices (menyalahgunakan peralatan komputer).
- 2).Kejahatan Dunia Maya yang menggunakan komputer sebagai alat kejahatan.
  - a). Credit card fraud (penipuan kartu kredit).
  - b). Bank fraud (penipuan terhadap bank).
  - c). Service Offered fraud (penipuan melalui penawaran suatu jasa).
  - d). Identity Theft and Fraud (pencurian identitas dan penipuan).
  - e). Computer-related fraud (penipuan melalui komputer).
  - f). Computer-related forgery (pemalsuan melalui komputer).
  - g). Computer-related betting (perjudian melalui komputer).
  - h). Computer-related Extortion and Threats (pemerasan dan pengancaman melalui komputer).
- 3).Kejahatan Dunia Maya yang berkaitan dengan isi atau muatan data atau sistem computer.
  - a). Child pornography (pornografi anak).
  - b). Infringements Of Copyright and Related Rights (pelanggaran terhadap hak cipta dan hak-hak terkait).
  - c). Drug Traffickers (peredaran narkoba).

Kegiatan siber meskipun bersifat virtual dapat dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Secara yuridis dalam hal ruang siber sudah tidak pada tempatnya lagi untuk kategorikan sesuatu dengan ukuran dalam kualifikasi hukum konvensional untuk dijadikan obyek dan perbuatan, sebab jika cara ini yang ditempuh akan terlalu banyak

---

<sup>2</sup> <http://www.scribd.com/doc/11654767/tinjauan-yuridis-pembuktian-cyber-crime-dalam-perspektif-hukum-positif-indonesia>, 21 November 2011, 15.00 wib.

kesulitan dan hal-hal yang lolos dari jerat hukum. Kegiatan siber adalah kegiatan virtual yang berdampak sangat nyata, meskipun alat buktinya bersifat elektronik. Dengan demikian, subyek pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata.<sup>3</sup>

Penggunaan hukum pidana dalam mengatur masyarakat pada hakekatnya merupakan bagian dari suatu langkah kebijakan. Selanjutnya untuk menentukan bagaimana suatu usaha yang rasional dalam melakukan kebijakan tidak dapat pula dipisahkan dari tujuan kebijakan pembangunan itu sendiri secara integral. Dengan demikian dalam usaha untuk menentukan suatu kebijakan apapun termasuk kebijakan hukum pidana selalu terkait dan tidak terlepas dari tujuan pembangunan nasional itu sendiri yakni bagaimana mewujudkan kesejahteraan bagi masyarakat.

Selain itu, perkembangan hukum di Indonesia terkesan lambat, karena hukum hanya akan berkembang setelah ada bentuk kejahatan baru. Jadi hukum di Indonesia tidak ada kecenderungan yang mengarah pada usaha preventif atau pencegahan melainkan usaha penyelesaiannya setelah terjadi suatu akibat hukum. Walaupun begitu proses perkembangan hukum tersebut masih harus mengikuti proses yang sangat panjang dan dapat dikatakan setelah negara menderita kerugian yang cukup besar hukum tersebut baru disahkan. Kebijakan hukum nasional kita yang kurang

---

<sup>3</sup> Pasal 5 Undang – undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Kementrian Komunikasi dan Informasi.



bisa mengikuti perkembangan kemajuan teknologi tersebut justru akan mendorong timbulnya kejahatan - kejahatan baru dalam masyarakat yang belum dapat dijerat dengan menggunakan hukum yang lama. Padahal negara sudah terancam dengan kerugian yang sangat besar namun tidak ada tindakan yang cukup cepat dari para pembuat hukum di Indonesia untuk mengatasi masalah tersebut.

#### B. Rumusan Masalah

Berdasarkan latar belakang masalah diatas, dapat diajukan beberapa permasalahan yang dapat menjadi pokok bahasan. Permasalahan - permasalahan tersebut apabila dirumuskan adalah sebagai berikut :

1. Bagaimanakah pelaksanaan Undang – Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE) terhadap tindak pidana Cyber crime?
2. Bagaimanakah sistem pembuktian tindak pidana Cyber crime dalam UU ITE?

#### C. Tujuan Penelitian

1. Mengetahui tentang pelaksanaan UU ITE terhadap tindak pidana Cyber crime.
2. Mengetahui tentang sistem pembuktian tindak pidana Cyber crime dalam UU ITE.

#### D. Manfaat Penelitian

##### 1. Manfaat Praktis

Peneliti berharap bahwa skripsi ini dapat memberikan pengetahuan kepada masyarakat untuk mengetahui pelaksanaan tindak pidana Cyber crime.

##### 2. Manfaat Teoritis

Sebagai referensi dan informasi di fakultas hukum dan diharapkan sebagai sumbangan pemikiran yang positif serta memberikan kontribusi untuk ilmu pengetahuan hukum, agar ilmu itu tetap hidup dan berkembang khususnya tentang tindak pidana Cyber crime.

#### E. Kajian Pustaka

##### 1. Pengertian Tindak Pidana

Tindak pidana berasal dari suatu istilah dalam hukum belanda yaitu strafbaarfeit. Ada pula yang mengistilahkan menjadi delict yang berasal dari bahasa latin delictum. Hukum pidana negara Anglo Saxon memakai istilah offense atau criminal act.

Menurut Moeljatno, perbuatan pidana adalah perbuatan yang dilarang oleh suatu aturan hukum larangan mana disertai ancaman (sanksi) yang berupa pidana tertentu, barang siapa melanggar larangan tersebut.<sup>4</sup> Larangan tersebut ditujukan pada perbuatan, sedangkan ancaman pidananya ditujukan pada orang yang menimbulkan kejadian itu. Moeljatno memisahkan antara criminal act dan criminal responsibility yang menjadi unsur tindak pidana. Menurut moeljatno hanya lah unsur –

---

<sup>4</sup> Moeljatno, Asas – Asas Hukum Pidana, Bina Aksara, Jakarta, 1987, h. 59

unsur yang melekat pada criminal act (perbuatan yang dapat di pidana). Sedangkan yang termasuk unsur – unsur tindak pidana adalah perbuatan yang memenuhi rumusan undang – undang bersifat melawan hukum.

Menurut Simons yang menggunakan istilah peristiwa pidana adalah perbuatan atau tindakan yang diancam dengan pidana oleh undang – undang bertentangan dengan hukum dan dilakukan oleh orang yang mampu bertanggung jawab.

Simon memandang semua syarat untuk menjatuhkan pidana sebagai unsur tindak pidana dan tidak memisahkan unsur yang melekat pada aliran tindak pidana (pertanggungjawaban pidana). Kemudian Simon menyebut unsur – unsur tindak pidana, yaitu perbuatan manusia diancam dengan pidana, melawan hukum, dilakukan dengan kesalahan, oleh orang yang mampu bertanggung jawab.

Unsur – unsur tersebut oleh Simon dibedakan antara unsur objektif dan unsur subjektif. Yang termasuk unsur objektif adalah perbuatan orang, akibat yang kelihatan dari perbuatan itu, dan kemungkinan adanya keadaan tertentu yang menyertainya. Unsur subjektif adalah orang yang mampu bertanggung jawab dan adanya kesalahan.

## 2. Pengertian Perspektif

Menurut kamus bahasa Indonesia pengertian dari perspektif adalah pandangan. Dalam skripsi ini yang dimaksud dengan perspektif adalah sudut pandang atau dilihat dari segi UU ITE.

### 3. Pengertian Komputer

Komputer terdiri atas dua bagian besar yaitu perangkat keras (hardware) dan perangkat lunak (software). Perangkat keras dari suatu komputer adalah wujud fisik dari suatu komputer yang dapat diraba dan dilihat. Perangkat keras antara lain berupa mesin, keyboard, mouse, dan lain – lain. Sementara itu perangkat lunak dari suatu komputer yang disebut juga sebagai program atau code, adalah perangkat yang memfungsikan atau menjalankan perangkat keras atau mesin komputer.<sup>5</sup>

### 4. Sejarah dan pengertian internet

Sejarah dan perkembangan internet tidak bisa lepas dari perang dingin antara Uni Soviet (USSR) dan Amerika Serikat yang mulai mengemuka sejak usainya Perang Dunia II. Uni Soviet memulai Perang Dingin dalam bidang teknologi dengan meluncurkan sputnik, satelit bumi buatan yang pertama pada 1957. Sebagai respon atas stimulus yang diberikan oleh Uni Soviet, Amerika Serikat membentuk Advance Research Project Agency (ARPA) pada tahun 1958. Dibentuknya ARPA menjadikan Department of Defense Amerika Serikat memimpin dalam pemanfaatan ilmu pengetahuan dan teknologi yang diterapkan dalam bidang militer.<sup>6</sup> Internet merupakan hasil pemikiran yang visioner dari sejumlah pakar pada permulaan 1960-an. Mereka melihat adanya nilai potensial apabila komputer dapat digunakan untuk berbagi informasi mengenai hasil penelitian dan pengembangan di bidang keilmuan dan militer. J.C.R.

---

<sup>5</sup> Sutan Remy Syahdeini, *Kejahatan Dan Tindak Pidana Komputer*, PT Pustaka Utama Grafiti, Jakarta, 2009, h. 30

<sup>6</sup> Agus Raharjo, *Cybercrime*, PT Citra Aditya Bakti, Bandung, 2000, h. 61.

Licklider dari MIT adalah yang pertama yang menyarankan agar dibangun suatu jaringan global internet (global network of computer) pada 1962. Licklider akhirnya pindah ke Defense Advance Projects Agency (DARPA) pada akhir 1962 untuk memimpin tugas mengembangkan pemikirannya itu.

Leonard Kleinrock dari MIT mengembangkan teori yang dikenal sebagai Theory of Packet Switching. Teori ini dimaksudkan untuk membangun dasar bagi hubungan – hubungan internet. Lawrence Robert dari MIT berhasil menghubungkan komputer di Massachusetts dengan suatu komputer di California pada 1965 melalui jalur telepon dial up. Hal yang dilakukan oleh Lawrence tersebut di satu pihak menunjukkan dimungkinkannya dibangun suatu Wide Area Networking tetapi di pihak lain juga menunjukkan bahwa telephone line's circuit switching dapat digunakan untuk membangun hubungan – hubungan komputer secara lebih luas. Dengan demikian Theory of Packet Switching memperoleh konfirmasi.

Internet yang kemudian dikenal ARPANET berhasil online pada tahun 1969 berdasarkan suatu kontrak yang dibuat oleh Advance Research Projects Agency (ARPA). Pada mulanya baru menghubungkan 4 buah komputer utama pada beberapa universitas di bagian south western Amerika Serikat, yaitu UCLA, Stanford Research Institute, UCSB, dan University Of Utah kontrak tersebut dilaksanakan oleh BBN Of Cambridge, MA di bawah Bob Kahn dan menjadi online pada Desember 1969. Pada Juni 1970, MIT, Harvard, BBN, dan System Development Corp. (SDC) di Santa Monica, California bergabung pula. Pada Januari 1971, menyusul

bergabung Stanford, Lincoln Labs dari MIT, Carmegie – mellon dan Case western Reserve Universty, pada bulan – bulan berikutnya NASA/ Ames, Mitre, Burrough, RAND, dan Universty of Illinois bergabung. Setelah itu bergabung banyak lagi institusi yang tentu saja tidak mungkin ditulis nama – namanya.<sup>7</sup>

Pada awalnya internet hanya menawarkan layanan berbasis text saja meliputi remote access, e-mail/ messaging, maupun diskusi melalui news group. Indonesia baru bisa menikmati layanan internet komersial pada sekitar tahun 1994. Sebelumnya, beberapa perguruan tinggi seperti Universitas Indonesia terlebih dahulu tersambung dengan jaringan internet melalui gateway yang menghubungkan universitas dengan network diluar negeri. Dunia internet merupakan sebuah tempat dimana kita hidup secara maya (virtual) dalam dunia ini kita dapat melakukan beberapa kegiatan yang mirip dengan kegiatan di dunia nyata. Kita dapat melakukan perniagaan atau sekedar sosialisasi.

Dunia maya ini juga memiliki aturan yang kita definisi kan bersama. Aturan ini ada yang sama dan ada yang berbeda dengan aturan yang ada di dunia nyata dikarenakan hukum – hukum fisika yang tidak berlaku di dunia ini dua orang yang secara fisik berada ditempat yang jaraknya ribuan kilometer dapat berada diruang virtual yang sama. Aturan yang sama antara lain sopan santun dan etika berbicara (menulis) meskipun kadang – kadang disertai dengan implementasi yang berbeda. Misalnya ketika kita menuliskan email dengan huruf besar semua, maka

---

<sup>7</sup> Sutan Remy Syahdeini, *Kejahatan dan tindak pidana komputer*, PT Pustaka Utama Grafiti, Jakarta, 2009, h. 9.

ini menandakan kita sedang marah. Sama ketika kita sedang berbicara dengan berteriak – teriak, maka kita dianggap sedang marah (padahal mungkin saja karakter kita memang begitu). Semua ini memiliki aturan yang di definisikan bersama.

Hal itu mengisyaratkan bahwa dunia maya yang di bangun atau di kontruksi melalui jaringan internet dapatlah membangun daya rangsang dan emosi besar penggunanya. Di satu sisi, pengguna internet dapat memenuhi kepuasan psikologisnya ketika problem yang di hadapinya dapat diselesaikan dengan jasa internet.

Internet telah mengkontruksikan dunia maya, yang sebenarnya (dalam praktiknya) menjadi dunia tanpa batas, dunia kebebasan, yang bisa dimasuki dan dimanfaatkan oleh siapapun.

Internet adalah jaringan luas dari komputer yang lazim disebut dengan Worldwide network. Internet merupakan jaringan komputer yang terhubung satu sama lain melalui media komunikasi, seperti kabel telepon, serat optik, satelit ataupun gelombang frekuensi. Jaringan komputer ini dapat berukuran kecil seperti Lokal Area Network (LAN) yang biasa dipakai secara intern di kantor-kantor, bank atau perusahaan atau biasa disebut dengan intranet, dapat juga berukuran superbesar seperti internet.<sup>8</sup>

Sementara The US Supreme Court mendefinisikan internet sebagai International Network Of Interconnected Computer, artinya jaringan internasional dari komputer-komputer yang saling hubungan.<sup>9</sup>

---

<sup>8</sup> Agus Raharjo, Cybercrime, PT Citra Aditya Bakti, Bandung, 2002, h. 59.

<sup>9</sup> Abdul Wahid dan Mohammad Labib, Kejahatan Mayantara, Refika Aditama , Bandung, 2010, h. 31.

Internet didefinisikan sebagai jaringan komputer yang menghubungkan situs akademik, pemerintah, komersil, organisasi maupun perorangan. Dalam definisi ini tampak bahwa internet mencakup juga terhadap jaringan yang biasa LAN (Local Area Network) dan WAN (Wide Area Network).<sup>10</sup>

5. Pengertian Informasi, Transaksi Elektronik dan Dokumen Elektronik menurut Undang – Undang No. 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Dalam ketentuan umum pasal 1 undang – undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik bahwa disebutkan pengertian Informasi Elektronik, Transaksi Elektronik Dan Dokumen Elektronik :

- a. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, Elektronik Data Interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
- b. Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya.
- c. Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.<sup>11</sup>

---

<sup>10</sup> Ibid. h. 31.

<sup>11</sup> Pasal 1 Undang – undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Kementerian Komunikasi dan Informasi.



## 6. Pengertian Pembuktian Dan Hukum Pembuktian

Pembuktian adalah suatu daya upaya para pihak yang berperkara untuk meyakinkan hakim tentang kebenaran dalil - dalil yang dikemukakannya di dalam suatu perkara yang sedang diperseketakan di muka pengadilan, atau yang diperiksa oleh hakim. Membuktikan artinya mempertimbangkan secara logis kebenaran suatu fakta atau peristiwa berdasarkan alat-alat bukti yang sah dan menurut hukum pembuktian yang berlaku. Dari pengertian tersebut, maka sudah dapat disimpulkan bahwa pembuktian adalah upaya para pihak yang berperkara untuk meyakinkan hakim akan kebenaran peristiwa atau kejadian yang di ajukan oleh para pihak yang bersengketa dengan alat - alat bukti yang telah ditetapkan oleh undang – undang.<sup>12</sup>

Hukum pembuktian adalah merupakan sebagian dari hukum acara pidana yang mengatur macam – macam alat bukti yang sah menurut hukum, sistem yang dianut dalam pembuktian, syarat – syarat dan tata cara mengajukan bukti tersebut serta kewenangan hakim untuk menerima, menolak, dan menilai suatu pembuktian.<sup>13</sup>

Sumber hukum pembuktian adalah undang – undang, doktrin, ajaran dan jurisprudensi. Karena hukum pembuktian adalah bagian dari hukum acara pidana, maka sumber hukum yang pertama adalah undang – undang nomor 8 tahun 1981 tentang hukum acara pidana atau KUHP. Lembaran Negara Republik Indonesia tahun 1981 nomor 76 dan

---

<sup>12</sup> <http://www.scribd.com/doc/11654767/tinjauan-yuridis-pembuktian-cyber-crime-dalam-prespektif-hukum-positif-indonesia>, 21 November 2011, 15.00 wib.

<sup>13</sup> Hari Sasangka dan Lily Rosita, *Hukum Pembuktian Dalam Perkara Pidana*, Mandar Maju, Bandung, 2003, h. 10

penjelasannya dimuat dalam tambahan Lembaran Negara Republik Indonesia nomor 3209.<sup>14</sup>

## 7. Pengertian Alat Bukti Menurut KUHAP dan UU ITE

Dalam KUHAP hakim tidak boleh menjatuhkan pidana kepada seorang kecuali apabila dengan sekurang – kurangnya dengan dua alat bukti yang sah yang memperoleh keyakinan bahwa suatu tindak pidana benar – benar terjadi dan bahwa terdakwa yang bersalah melakukannya sesuai dengan pasal 183. Dalam UU ITE pasal 5 ayat (1) dan (2) mendiskripsikan bahwa dokumen elektronik dan transaksi elektronik adalah alat bukti yang sah. Selain dalam undang – undang yang sama pasal 44 mengatakan :

- a. alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan; dan
- b. alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3).

## 8. Sejarah dan Pengertian Cyber crime

Pesatnya perkembangan di bidang teknologi informasi saat ini merupakan dampak dari semakin kompleksnya kebutuhan manusia akan informasi itu sendiri. Adanya hubungan antara informasi dan teknologi jaringan komunikasi, telah menghasilkan dunia maya yang amat luas yang biasa disebut dengan teknologi cyberspace. Teknologi ini memuat kumpulan informasi yang dapat diakses oleh semua orang dalam bentuk jaringan-jaringan komputer yang disebut jaringan internet. Sebagai media penyedia informasi internet juga merupakan sarana kegiatan komunitas

---

<sup>14</sup> Hari Sasangka dan Lily Rosita, Hukum Pembuktian Dalam Perkara Pidana, Mandar Maju, Bandung, 2003, h. 10

komersial terbesar dan terpesat pertumbuhannya. Sistem jaringan memungkinkan setiap orang dapat mengetahui dan mengirimkan informasi secara cepat dan menghilangkan batas-batas teritorial suatu wilayah negara. Kepentingan yang ada tidak lagi sebatas kepentingan suatu bangsa semata, melainkan juga kepentingan regional bahkan internasional.

Perkembangan teknologi informasi yang terjadi pada hampir setiap negara sudah merupakan ciri global yang mengakibatkan hilangnya batas-batas negara. Setiap negara harus menghadapi kenyataan bahwa informasi dunia saat ini dibangun berdasarkan suatu jaringan yang ditawarkan oleh kemajuan bidang teknologi. Salah satu cara berpikir yang produktif adalah mendirikan usaha untuk menyediakan suatu infra struktur informasi yang baik di dalam negeri, yang kemudian dihubungkan dengan jaringan informasi global.

Kecenderungan mengglobalnya karakteristik teknologi informasi yang semakin memanjakan pemakainya dengan kemudahan mengakses, akhirnya menjadikan Indonesia harus mengikuti pola tersebut. Bentuk kejahatan (crime) secara otomatis akan mengikuti untuk kemudian beradaptasi pada tingkat perkembangan teknologi. Contoh terbesar saat ini adalah kejahatan maya atau biasa disebut Cyber crime. Merupakan bentuk fenomena baru dalam tindak kejahatan sebagai dampak langsung dari perkembangan teknologi informasi. Terdapat beberapa sebutan yang diberikan pada jenis kejahatan baru ini, antara lain: sebagai kejahatan dunia maya (cyber-space/ virtual - space offence), dimensi baru dari hi-

tech crime, dimensi baru dari transnational crime, dan dimensi baru dari white collar crime.

Hacker muncul pada awal tahun 1960-an diantara para anggota organisasi mahasiswa Tech Model Railroad Club di Laboratorium Kecerdasan Artifisial Massachusetts Institute of Technology (MIT). Kelompok mahasiswa tersebut merupakan salah satu perintis perkembangan teknologi komputer dan mereka beroperasi dengan sejumlah komputer mainframe. Kata Hacker pertama kali muncul dengan arti positif untuk menyebut seorang anggota yang memiliki keahlian dalam bidang komputer dan mampu membuat program komputer yang lebih baik dari yang telah dirancang bersama. Kemudian pada tahun 1983, analogi Hacker semakin berkembang untuk menyebut seseorang yang memiliki obsesi untuk memahami dan menguasai sistem komputer. Pasalnya, pada tahun tersebut untuk pertama kalinya FBI menangkap kelompok kriminal komputer The 414s yang berbasis di Milwaukee AS. 414 merupakan kode area lokal mereka. Kelompok yang kemudian disebut Hacker tersebut dinyatakan bersalah atas pembobolan 60 buah komputer, dari komputer milik Pusat Kanker Memorial Sloan - Kettering hingga komputer milik Laboratorium Nasional Los Alamos. Salah seorang dari antara pelaku tersebut mendapatkan kekebalan karena testimonialnya, sedangkan 5 pelaku lainnya mendapatkan hukuman masa percobaan.

Perkembangan internet dapat dirunut dari peristiwa peluncuran pesawat Sputnik milik Uni Soviet yang ditanggapi oleh Amerika Serikat dengan membuat proyek peluncuran pesawat luar angkasa. Untuk

kepentingan pesawat luar angkasa itu dibangunlah suatu jaringan informasi yang memang diperlukan untuk mengoperasikannya. Pada awalnya jaringan sistem informasi yang dibuat untuk lingkup lokal yang tertutup atau yang dikenal sebagai Local Area Network /LAN.

Pada tahun 1977, ada dua orang anak muda kreatif Steve Jobs dan Steve Wozniak. Mereka memperkenalkan konsep baru personal komputer yang diberi nama Apple computer Generasi I. Sekitar awal tahun 1990-an, LAN pun kemudian digunakan untuk kepentingan kekuasaan khususnya kepentingan militer bagi Amerika Serikat. LAN kemudian dikembangkan secara terbatas menjadi Wide Area Network (WAN), untuk kemudian menjadi suatu sistem dengan berbagai mesin informasi yang luar biasa seperti yang kemudian dikenal sebagai internet. Memasuki abad 21, memudarnya batas-batas geografis membuat paradigma - paradigma penyelesaian dan praktik kejahatan lama menjadi tidak terpakai lagi. Kekuatan jaringan dan personal komputer berbasis Pentium menjadikan setiap komputer sebagai alat yang potensial bagi para pelaku kejahatan. Globalisasi aktivitas kriminal yang memungkinkan para penjahat melintas batas elektronik merupakan masalah nyata dengan potensi mempengaruhi setiap negara, hukum dan warga negara.

Dunia maya menghasilkan sisi gelap dalam bentuk kejahatan, yang disebut Cyber crime. Perkembangan teknologi informasi telah mengubah cara pandang sebagian pelaku ekonomi beraktivitas, khususnya dalam bentuk dunia bisnis. Sistem teknologi informasi tidak hanya berfungsi sebagai sarana peningkatan kualitas, efisiensi dan produktivitas

kerja, tetapi telah menjadi senjata untuk mengambil keuntungan secara cepat dengan jalan illegal, khususnya penggunaan internet. Pada awal Maret 2002, Gartner Inc. ([www.gartner.com](http://www.gartner.com)) menyatakan bahwa lebih dari US\$ 700.000.000 nilai transaksi via internet hilang sepanjang tahun 2001 akibat Cyber Fraud.

Apabila berbicara tentang jaringan komputer yang bernama internet, menurut kongres PBB ke-10 di Wina, Austria, ada tiga hal yang paling penting pada sistem komputer dan keamanan data, yaitu : assurance confidentiality, integrity or availability of data dan processing function.

Pada masa-masa awal, kemajuan teknologi komunikasi dan informasi pada umumnya dan internet pada khususnya tidak bisa dinikmati secara luas seperti sekarang. Tetapi hanya dapat digunakan dan untuk memfasilitasi kepentingan para elit saja. Seiring dengan perjalanan waktu, para industriawan berhasil mengaplikasikan internet untuk keperluan industri. Dengan kata lain, penaklukan antar negara bukan hanya sebatas memperluas wilayah. Melainkan juga penguasaan sumber-sumber bagi mesin industri Selain itu, penguasaan pengetahuan dan teknologi yang kemudian diterapkan di dalam dunia industri terutama pasca Perang Dingin. Internet tidak lagi semata digunakan untuk kepentingan militer, tetapi beralih fungsi menjadi sebuah media massa yang mampu membawa perubahan dalam kehidupan manusia.

Internet mulai digunakan sebagai alat propaganda politik, transaksi bisnis atau perdagangan, sarana pendidikan, kesehatan, manufaktur, perancangan, pemerintah, prostitusi, pornografi dan

kejahatan. Internet telah memberikan cakrawala baru dalam kehidupan manusia. Internet membawa kita kepada ruang atau dunia baru yang tercipta yang dinamakan Cyberspace. Cyberspace merupakan tempat seseorang berada pada waktu yang bersangkutan sedang mengarungi dunia informasi global interaktif yang bernama internet. Cyber crime merupakan kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet.

Kejahatan yang lahir sebagai dampak negatif dari perkembangan aplikasi internet ini sering disebut Cyber crime menurut Ari Juliano Gema (2000)<sup>15</sup>.

Menurut kepolisian Inggris, Cyber crime adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital.<sup>16</sup>

Kejahatan dunia maya adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan di akses oleh pelanggan internet itu.<sup>17</sup>

Dalam laporan kongres PBB X/2000 dinyatakan Cyber crime atau komputer – related crime, mencakup keseluruhan bentuk – bentuk

---

<sup>15</sup> Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara*, Refika Aditama, Bandung, 2010 h. 39

<sup>16</sup> Ibid h. 40

<sup>17</sup> Ibid h. 40

baru dari kejahatan yang ditujukan kepada komputer, jaringan komputer, dan para penggunanya, dan bentuk – bentuk kejahatan tradisional yang sekarang dilakukan dengan menggunakan atau dengan bantuan peralatan komputer.<sup>18</sup>

#### 9. Proses Hacking sebagai Cyber crime

Perkembangan teknologi informasi telah mengubah hampir semua sisi kehidupan. Pada satu sisi teknologi komputer memberikan keuntungan berupa kesempatan untuk mendapatkan informasi, pekerjaan, berpartisipasi dalam politik dan kehidupan berdemokrasi serta keuntungan lain. Akan tetapi pada sisi lain ia akan semakin menggrogoti kehidupan nyata yang telah lama kita geluti dengan segala peninggalan yang harus dipecahkan sebelum ia bergerak lebih jauh menyusuri jalan dan lorong – lorong Cyberspace.

Bagi mereka yang memanfaatkan teknologi informasi ini untuk kegiatan bisnis, pelayanan publik dan media hiburan dengan membangun situs – situs yang dapat dikunjungi oleh masyarakat. Tetapi harus berhati – hati karena tidak semua masyarakat yang berkunjung ke dunia maya menikmati realitas virtual yang ditawarkan pada situs itu. Seperti halnya dalam kehidupan nyata disana juga ada kejahatan yang dampaknya akan dirasakan dalam kehidupan nyata.

Hacking merupakan salah satu kegiatan yang bersifat negatif, meskipun awalnya Hacking memiliki tujuan mulia yaitu untuk memperbaiki sistem keamanan yang telah dibangun dan memperkuatnya.

---

<sup>18</sup> Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara*, Refika Aditama, Bandung, 2010 h. 41



Tetapi dalam perkembangannya Hacking digunakan untuk keperluan – keperluan lain yang bersifat merugikan. Hal ini tidak lepas dari pengguna internet yang semakin meluas sehingga penyalahgunaan kemampuan Hacking juga mengikuti luasnya pemanfaatan internet.

Beberapa tahap Hacking yang selanjutnya akan digunakan sebagai langkah untuk menentukan tahap – tahap Hacking yang dapat dikategorikan sebagai kejahatan. Tahap – tahap Hacking seperti yang dimaksud adalah :

- a. Mengumpulkan dan mempelajari informasi yang ada mengenai sistem operasi komputer atau jaringan komputer yang dipakai pada target sasaran.
- b. Menyusup atau mengakses jaringan komputer target sasaran.
- c. Menjelajahi sistem komputer dan mencari akses yang lebih tinggi.
- d. Membuat backdoor dan menghilangkan jejak.

Hacker harus memiliki pengetahuan dan kemampuan menguasai serta mengaplikasikan bahasa pemrograman. Pengetahuan dan kemampuan itu dapat diperoleh dengan berbagai cara diantaranya dengan belajar pada ahlinya atau belajar sendiri secara otodidak. Bahasa pemrograman merupakan bahasa teknis, sehingga orang yang benar – benar tidak mempunyai kemampuan teknis akan kesulitan untuk memahami bahasa teknis ini.

Setiap sistem operasi mempunyai kelemahan. Kelemahan itu lambat laun akan diketahui oleh para Hacker melalui berbagai cara, diantaranya adalah mempelajari sistem operasi tersebut, diskusi dengan

sesama Hacker melalui mailing list, newsgroup maupun mengambil informasi dari sebuah situs di internet yang menyajikan informasi mengenai kelemahan – kelemahan sistem operasi komputer. Kemudahan memperoleh informasi mempermudah Hacker dapat mengetahui kelemahan sistem operasi tersebut.

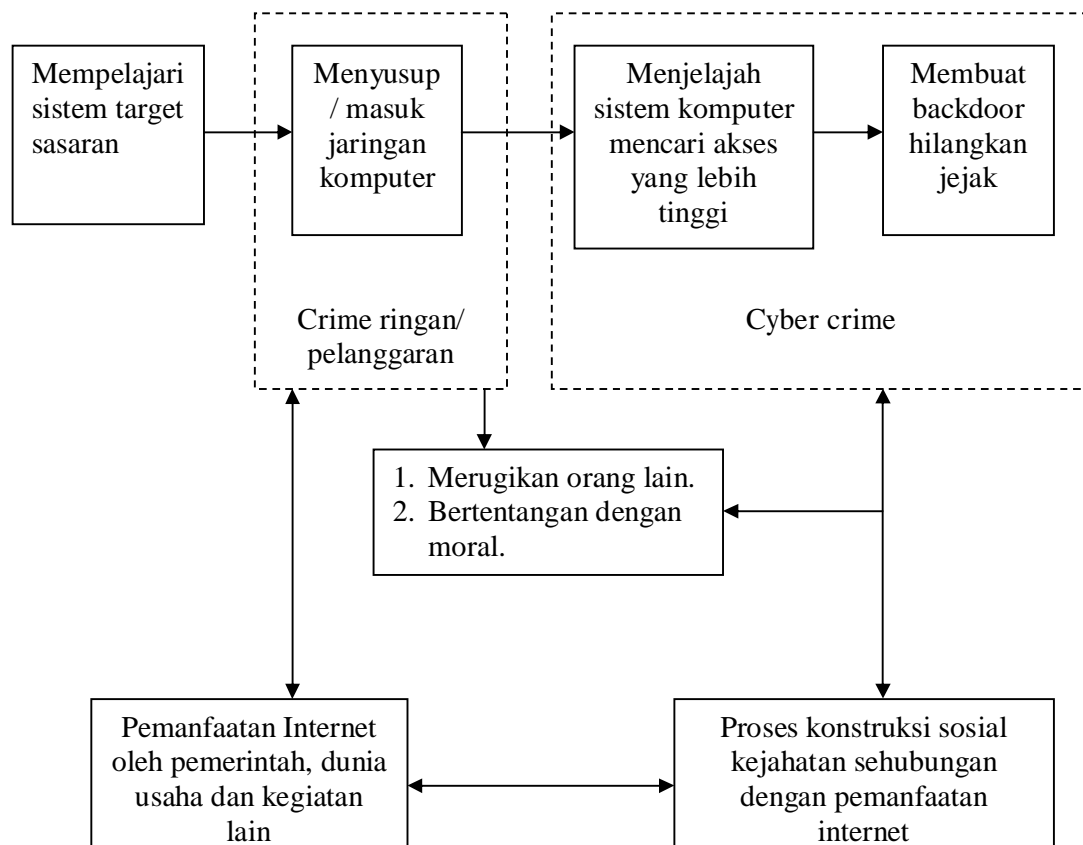
Berusaha untuk mengetahui sesuatu bukanlah kejahatan, mencari dan mengumpulkan informasi mengenai suatu sistem operasi yang digunakan pada sebuah perusahaan atau instansi pemerintah juga bukan merupakan kejahatan karena keingintahuan merupakan sifat yang manusiawi. Informasi adalah bebas, ia bergerak ke mana saja dan hak untuk mendapatkan informasi merupakan hak asasi yang dijamin dengan undang – undang. Pembatas atau larangan terhadap kebebasan mendapatkan informasi merupakan halangan untuk menumbuhkan daya kreatifitas dan pengembangan ilmu pengetahuan dan teknologi. Kebebasan informasi yang dipegang teguh oleh seorang Hacker.

Langkah Hacker setelah mengetahui sistem operasi apa yang dipakai pada target sasaran adalah menyusup atau mengakses jaringan komputer target sasaran itu. Menyusup atau mengakses jaringan komputer target sasaran ini dilakukan dengan mengeksploitasi kelemahan yang ada pada sistem operasi tersebut. Dengan kata lain Hacker memasuki situs orang lain tanpa izin. Hacker dengan kemampuannya dapat masuk dan berjalan – jalan dalam situs orang lain meskipun situs itu telah dilengkapi dengan sistem keamanan. Tantangan bagi para Hacker adalah membongkar sistem yang digunakan oleh pemilik situs tersebut. Jika

langkah ini dapat dilakukan maka merupakan kebanggaan tersendiri bagi Hacker, setidak – tidaknya merupakan modal untuk mendapatkan pengakuan mengenai status dirinya dari sesama Hacker.

Hacker yang sudah bisa memasuki situs orang lain merupakan kejahatan Cyber crime karena situs merupakan ruang privat orang yang membuat situs tersebut. Dengan mengacak – acak tampilan yang jauh dari aslinya dan menghapus file – file yang ada di situs tersebut sudah bukan rasa keingintahuan biasa yang dimiliki orang hal ini sudah termasuk dalam kejahatan.

Skema Proses Hacking jadi Kejahatan (Cyber crime)



Sumber : Agus Raharjo, Cybercrime, PT Citra Aditya Bakti, Bandung, 2002, h.199.

## 10. Bentuk – Bentuk Cyber crime

Berdasarkan jenis aktifitas yang dilakukannya, Cyber crime dapat digolongkan menjadi beberapa jenis sebagai berikut<sup>19</sup>:

### a. Unauthorized Access

Merupakan kejahatan yang terjadi ketika seseorang memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Probing dan port merupakan contoh kejahatan ini.

### b. Illegal Contents

Merupakan kejahatan yang dilakukan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum, contohnya adalah penyebaran pornografi.

### c. Penyebaran virus secara sengaja

Penyebaran virus pada umumnya dilakukan dengan menggunakan email. Sering kali orang yang sistem emailnya terkena virus tidak menyadari hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya.

### d. Data Forgery

Kejahatan jenis ini dilakukan dengan tujuan memalsukan data pada dokumen - dokumen penting yang ada di internet. Dokumen-dokumen ini biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis web database.

### e. Cyber Espionage, Sabotage, and Extortion

Cyber Espionage merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata - mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran. Sabotage and Extortion merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

### f. Cyberstalking

Kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya menggunakan e-mail dan dilakukan berulang - ulang. Kejahatan tersebut menyerupai teror yang ditujukan kepada seseorang dengan memanfaatkan media internet. Hal itu bisa terjadi karena kemudahan

---

<sup>19</sup> <http://www.scribd.com/doc/11654767/tinjauan-yuridis-pembuktian-cyber-crime>  
– dalam – perspektif – hukum – positif – indonesia, 21 November 2011, 15.00 wib.

dalam membuat email dengan alamat tertentu tanpa harus menyertakan identitas diri yang sebenarnya.

g. Carding

Carding merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet.

h. Hacking dan Cracker

Istilah Hacker biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Adapun mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut cracker. Boleh dibilang cracker ini sebenarnya adalah Hacker yang memanfaatkan kemampuannya untuk hal-hal yang negatif. Aktivitas cracking di internet memiliki lingkup yang sangat luas, mulai dari pembajakan account milik orang lain, pembajakan situs web, probing, menyebarkan virus, hingga pelumpuhan target sasaran. Tindakan yang terakhir disebut sebagai DoS (Denial of Service). Dos attack merupakan serangan yang bertujuan melumpuhkan target (hang, crash) sehingga tidak dapat memberikan layanan.

i. Cybersquatting and Typosquatting

Cybersquatting merupakan kejahatan yang dilakukan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. Adapun typosquatting adalah kejahatan dengan membuat domain plesetan yaitu domain yang mirip dengan nama domain orang lain. Nama tersebut merupakan nama domain saingan perusahaan.

j. Hijacking

Hijacking merupakan kejahatan melakukan pembajakan hasil karya orang lain. Yang paling sering terjadi adalah Software Piracy (pembajakan perangkat lunak).

k. Cyber Teroris

Suatu tindakan Cyber crime termasuk Cyber Terrorism jika mengancam pemerintah atau warganegara, termasuk cracking ke situs pemerintah atau militer.

## F. Metode Penelitian

Penelitian hukum pada dasarnya merupakan suatu kegiatan ilmiah yang didasarkan pada metode, sistematika, dan pemikiran tertentu yang bertujuan untuk mempelajari satu atau beberapa gejala hukum tertentu dengan

jalan menganalisisnya, kecuali itu, maka juga diadakan pemeriksaan yang mendalam terhadap fakta hukum tersebut untuk kemudian mengusahakan suatu pemecahan atas permasalahan-permasalahan yang timbul didalam gejala bersangkutan.<sup>20</sup>

Penelitian merupakan suatu saran (ilmiah) bagi pengembangan ilmu pengetahuan dan teknologi, maka metodologi penelitian yang diterapkan harus senantiasa disesuaikan dengan ilmu pengetahuan yang menjadi induknya.<sup>21</sup>

## 1. Pendekatan Masalah

Menggunakan pendekatan normatif, tinjauan yuridis normatif yang dengan melakukan identifikasi terhadap isu – isu hukum yang kurang berkembang dalam masyarakat, mengkaji penerapan – penarapan hukum dalam masyarakat, mengkaji pendapat para ahli – ahli hukum terkait dan analisa kasus dalam dokumen – dokumen untuk memperjelas hasil penelitian kemudian ditinjau aspek praktis dan aspek akademis keilmuan hukumnya dalam penelitian hukum.

## 2. Sumber Bahan Hukum

### a. Sumber bahan hukum primer

Konsep – konsep hukum yang berkaitan dengan Cyber crime dan Cyber Law yang mengatur tentang tindak pidana virtual yang tercantum di dalam :

#### (1). UU ITE

---

<sup>20</sup> Sunggono, Bambang, Metodologi Penelitian Hukum, Rajawali Pers, Jakarta, 2010, hal. 38

<sup>21</sup> Soekanto, Suryono, Penelitian Hukum Normatif, PT. Raja Grafindo Persada, Jakarta, 2007, hal. 1

(2). KUHP

(3). KUHAP

b. Sumber bahan hukum sekunder

Bahan hukum yang diambil dari pendapat atau tulisan para ahli dalam bidang Cyber crime untuk digunakan dalam membuat konsep – konsep hukum yang berkaitan dengan penelitian ini dan dianggap sangat penting.

### 3. Pengumpulan Bahan Hukum

Dilakukan dengan melakukan penelusuran bahan hukum melalui alat bantu catatan untuk dapat digunakan sebagai landasan teoritis berupa pendapat atau tulisan para ahli sehingga dapat diperoleh informasi dalam bentuk ketentuan formal dan resmi oleh pihak yang berkompeten dalam bidang Cyber crime.

### 4. Teknik Analisis Data

Penelitian ini menggunakan pendekatan yuridis normatif yaitu dengan mengkaji literatur – literatur yang berkaitan, pendapat para ahli – ahli hukum terkait dan analisa kasus dalam dokumen – dokumen untuk memperjelas hasil penelitian. Selain itu juga digunakan pendekatan undang – undang terkait dengan Cyber crime yaitu undang – undang nomor 11 tahun 2008.

## G. Sistematika Penulisan

Skripsi ini nantinya akan disusun dalam empat bab. Tiap-tiap bab dibagi beberapa sub bab yang saling mendukung. Bab-bab yang tersusun tersebut nantinya merupakan suatu kesatuan yang saling berkaitan antara satu dengan yang lain.

Bab I, Pendahuluan. Didalamnya terdiri dari tujuh sub bab yaitu sub bab pertama menguraikan tentang latar belakang masalah, kemudian sub bab kedua menguraikan tentang perumusan masalah. Selanjutnya di sub bab ketiga disajikan tujuan dan sub bab keempat mengenai manfaat penelitian sebagai harapan yang ingin dicapai melalui penelitian ini. Pada bagian sub bab kelima mengenai kajian pustaka yang merupakan landasan teori dari penulisan skripsi. Kemudian diuraikan beberapa konsep definisi yang berkaitan dengan judul penelitian. Selanjutnya sub bab keenam diuraikan tentang metode penelitian yang merupakan salah satu syarat dalam setiap penelitian. Intinya mengemukakan tentang tipe penelitian, sumber bahan hukum, dan sub bab yang ketujuh merupakan sub bab terakhir ini diakhiri dengan sistematika penulisan.

Bab II, menguraikan tentang pelaksanaan UU ITE terhadap tindak pidana Cyber crime, secara umum bab ini terdapat tiga sub bab yakni yang pertama mengenai proses terjadinya Cyber crime, kemudian sub bab kedua mengenai prosedur penanganan ditingkat kepolisian, dan sub bab yang terakhir membahas mengenai analisa pelaksanaan UU ITE terhadap Tindak pidana Cyber crime.



Bab III, menguraikan tentang sistem pembuktian terhadap tindak pidana Cyber crime dalam UU ITE, dalam bab ini terdapat dua sub bab yang terdiri dari sub bab pertama mengenai proses pembuktian terhadap tindak pidana Cyber crime dan pada sub bab kedua membahas mengenai beberapa contoh Tindak Pidana Cyber crime.

Bab IV merupakan bab penutup yang terdiri dari dua sub bab, yaitu sub bab pertama mengenai kesimpulan dan sub bab kedua membahas tentang saran.